CSCI 3330 Cybersecurity

Word of the day

YAK SHAVING [MIT AI Lab, after 2000: orig. probably from a Ren & Stimpy episode.] Any seemingly pointless activity which is actually necessary to solve a problem which solves a problem which, several levels of recursion later, solves the real problem you're working on.

Agenda for today

- Recap CBC padding oracles
- Further delve into how symmetric and asymmetric cryptography are used together
- Take a look at RSA (an asymmetric algorithm)

Symmetric encryption

- Same key used to encrypt and decrypt

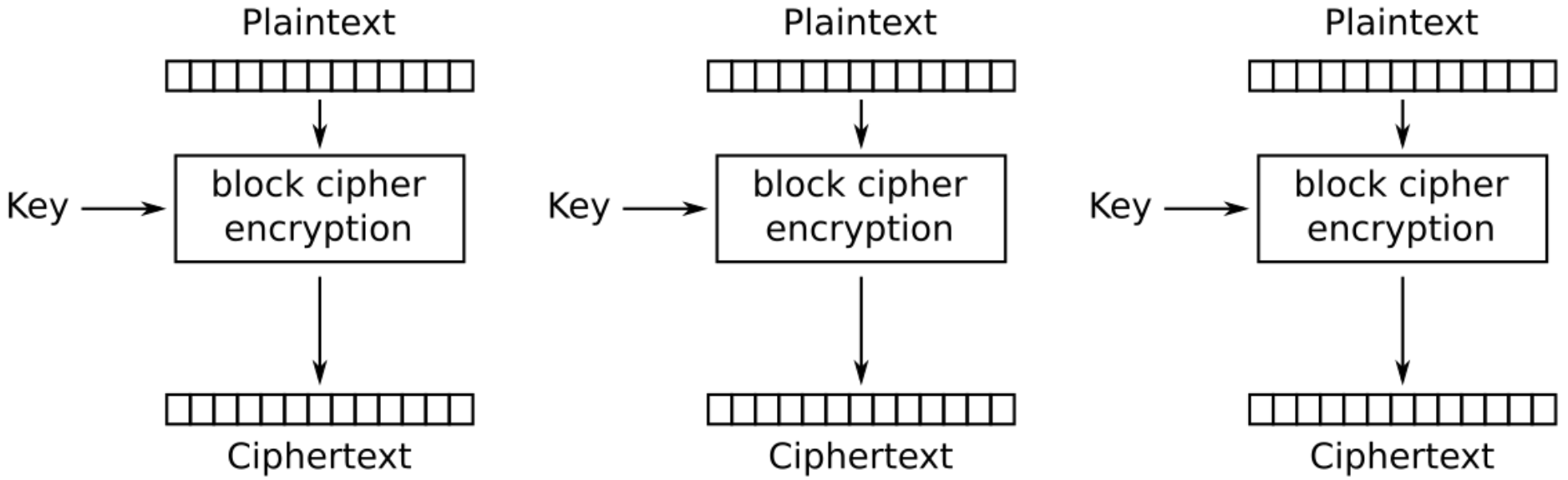
Common symmetric block ciphers

- DES
  - Data Encryption Standard
- AES
  - Advanced Encryption Standard

Block cipher modes

- Block ciphers encrypt/decrypt blocks
- Problem: my data is more than a block!
- Block cipher *modes*

ECB mode



Electronic Codebook (ECB) mode encryption

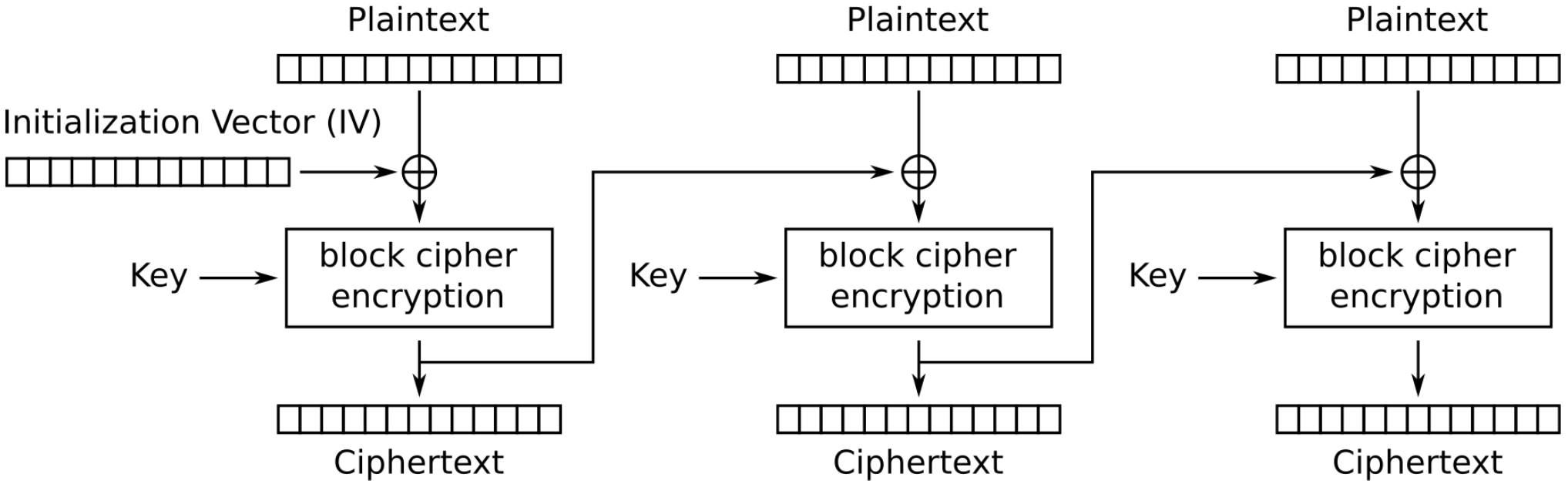
ECB mode

Original image

Using ECB allows patterns to be easily discerned

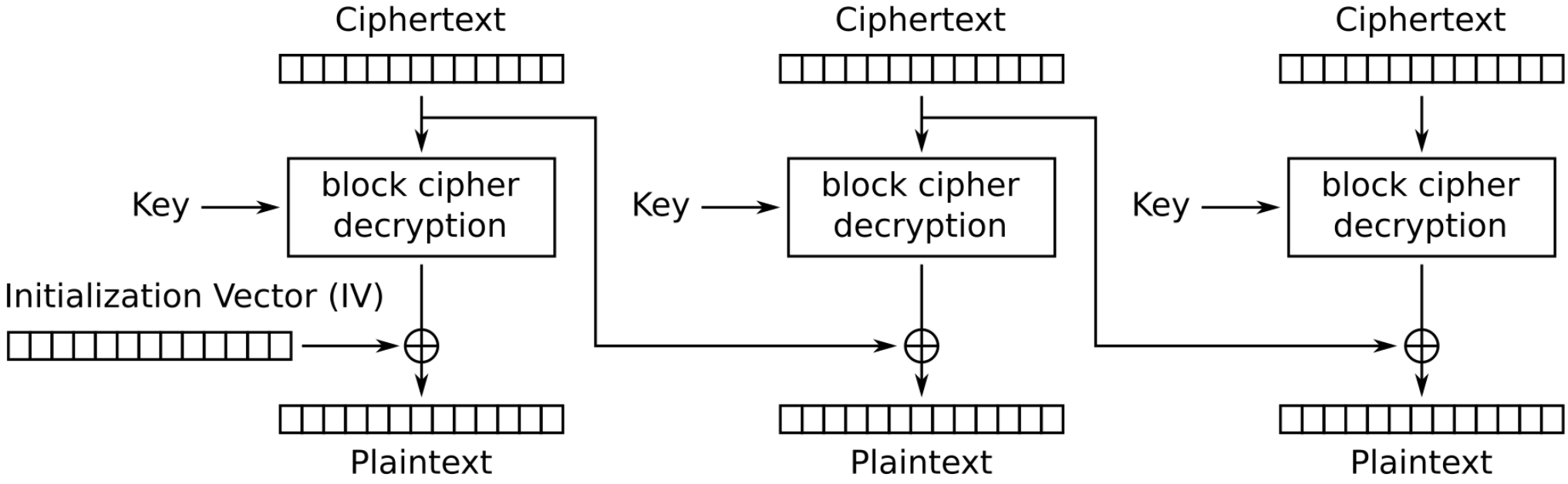
Modes other than ECB result in pseudo-randomness

CBC mode



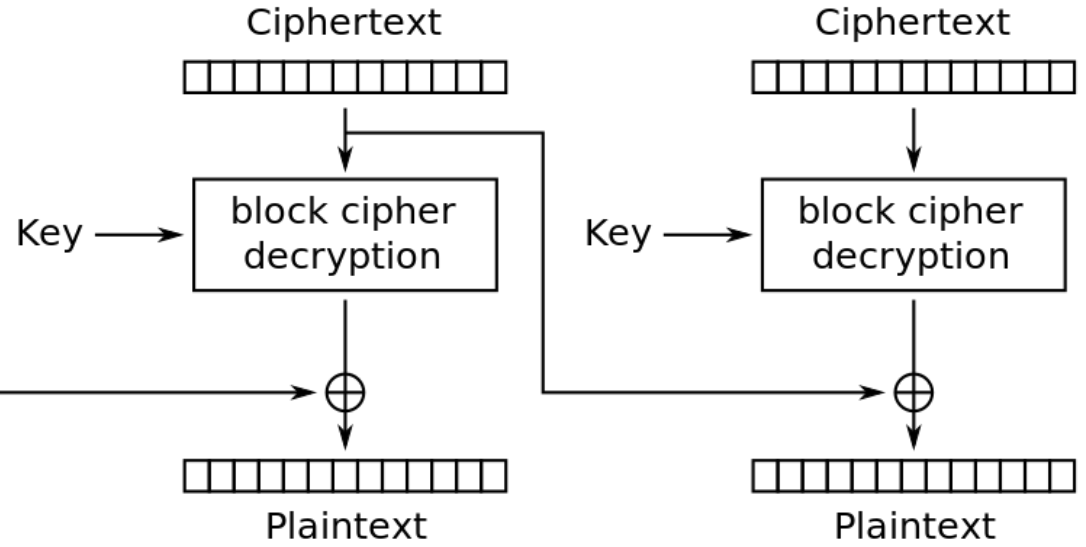
Cipher Block Chaining (CBC) mode encryption

CBC padding oracle



Cipher Block Chaining (CBC) mode decryption

CBC padding oracle



$$\text{ciphertext}_{n-1} \oplus \text{Decrypt}(\text{ciphertext}_n) = \text{plaintext}_n$$

Chaining (CBC) mode decryption

CBC padding oracle

Find byte *b* such that

$$b \oplus \text{Decrypt}(\text{ciphertext}_n)[15] == 0x01 \Rightarrow \text{Decrypt}(\text{ciphertext}_n)[15] == b \oplus 0x01$$

To recover $\text{plaintext}_n[15]$

$$\text{plaintext}_n[15] = \text{ciphertext}_{n-1}[15] \oplus b \oplus 0x01$$

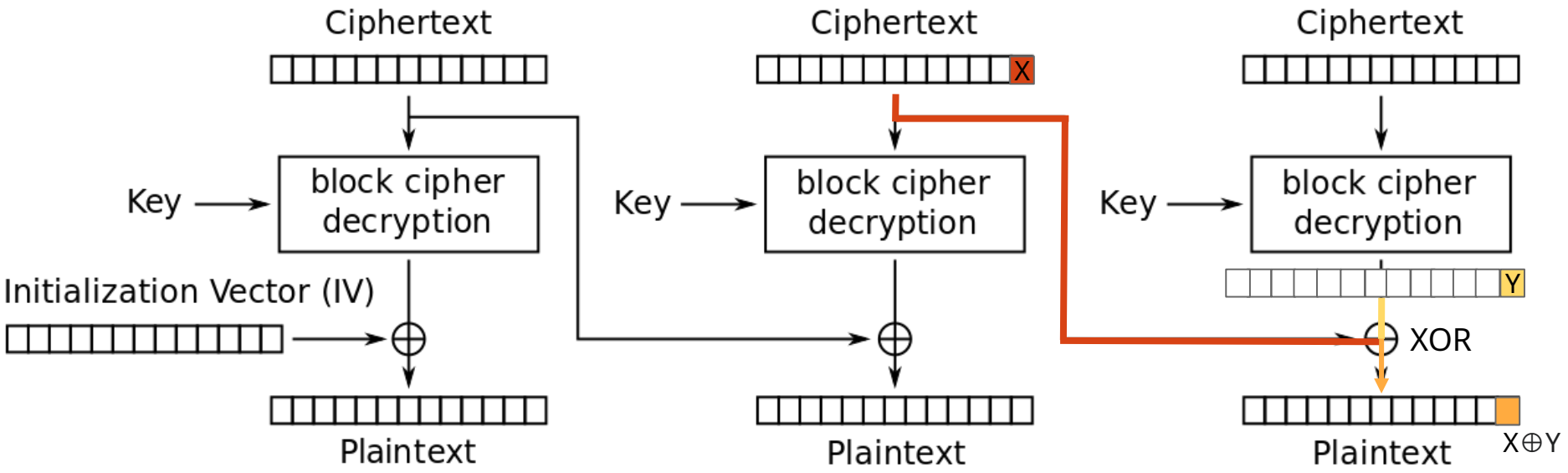
Set

$$\text{ciphertext}_{n-1}[15] = b \oplus 0x01 \oplus 0x02$$

Find *b* such that

$$b \oplus \text{Decrypt}(\text{ciphertext}_n)[14] == 0x02$$

…



Cipher Block Chaining (CBC) mode decryption

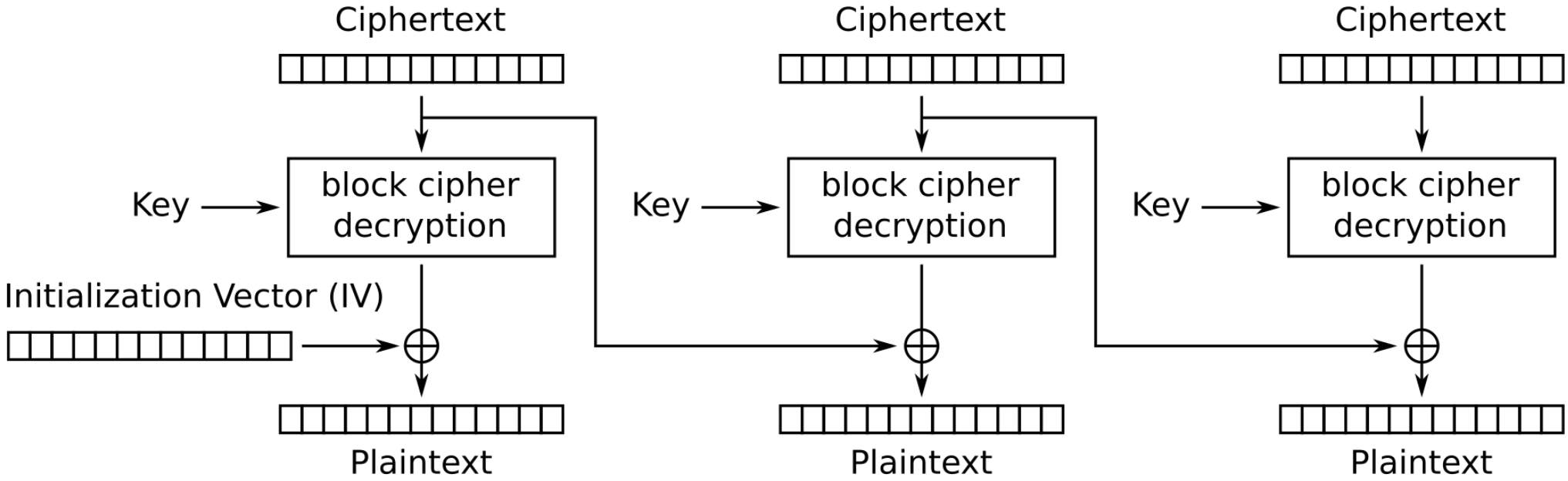
Padding Oracle Attack: changing the last byte of the penultimate ciphertext block changes the last byte of the final plaintext block.

There are only

256

possible bytes

CBC mode: error propagation



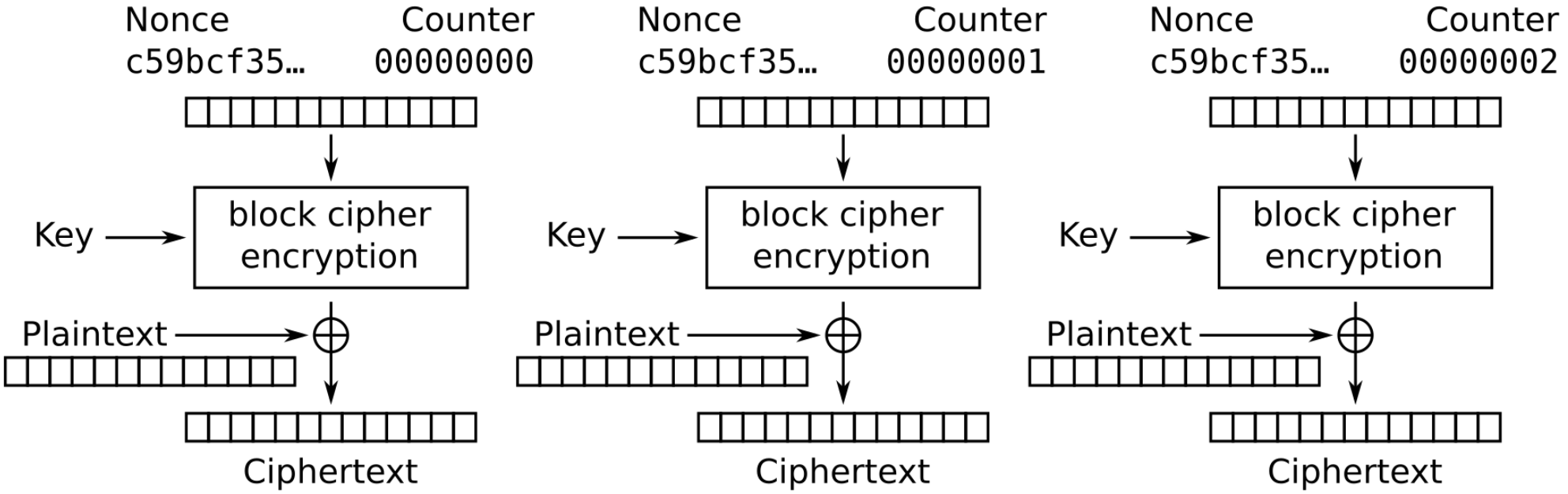
Cipher Block Chaining (CBC) mode decryption

An error in the ciphertext corrupts next block

CBC padding oracle attack

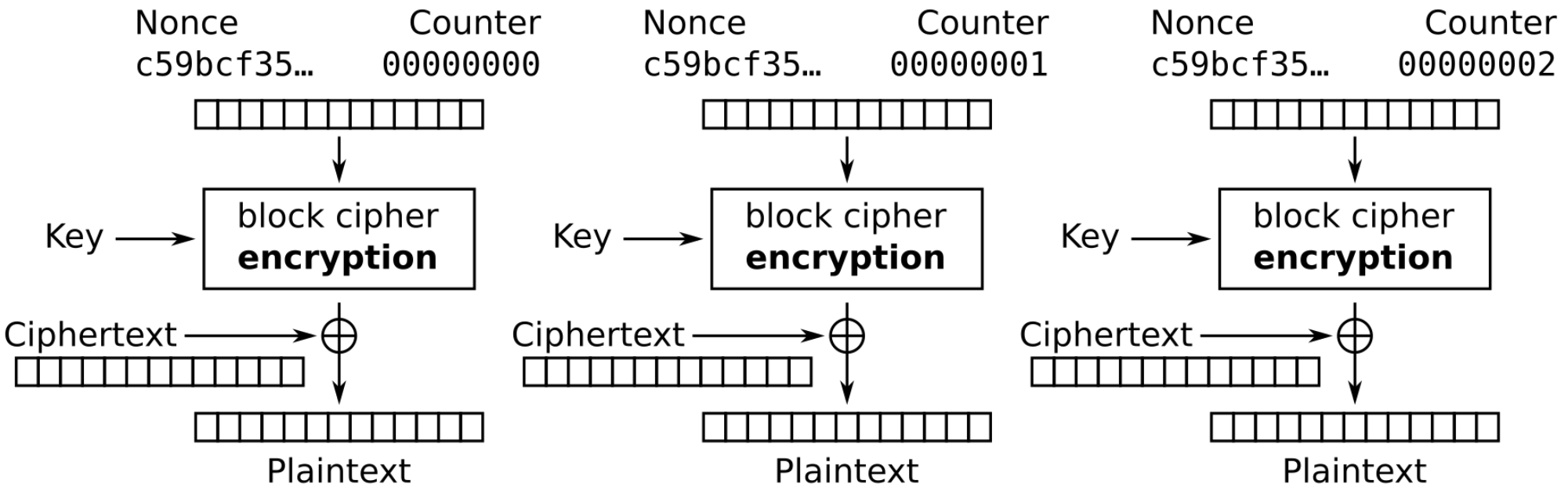
- Is it a chosen plaintext attack or a chosen ciphertext attack?
- What is the side-channel?

CTR mode



Counter (CTR) mode encryption

CTR mode



Counter (CTR) mode decryption

Parallelizable, no padding required!

GCM mode

- Combines counter mode with authentication (provides *integrity*)
- The mode considered “the best” (for now)

Problem with symmetric encryption

- I develop the new SnapTok app
- I want users to encrypt their uploads
- I embed an AES key into the app and the same key on my servers
- The user encrypts their uploads with this AES key
- Problem?

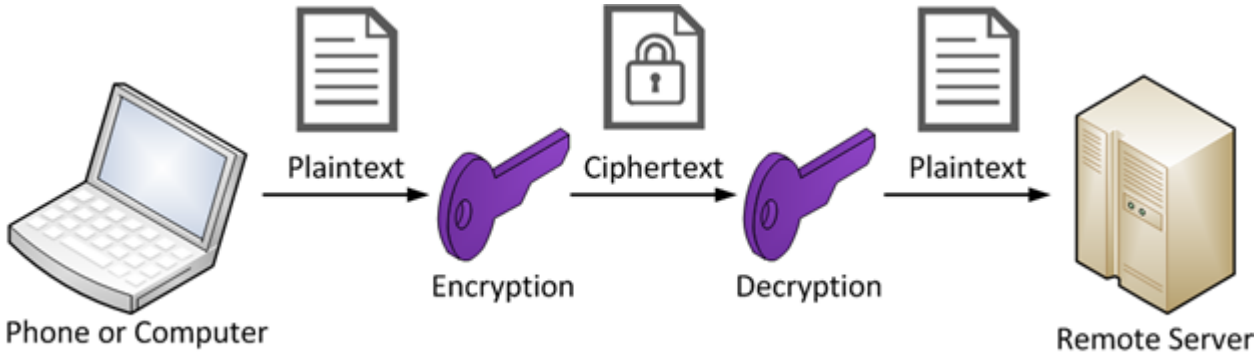
Problem with symmetric encryption

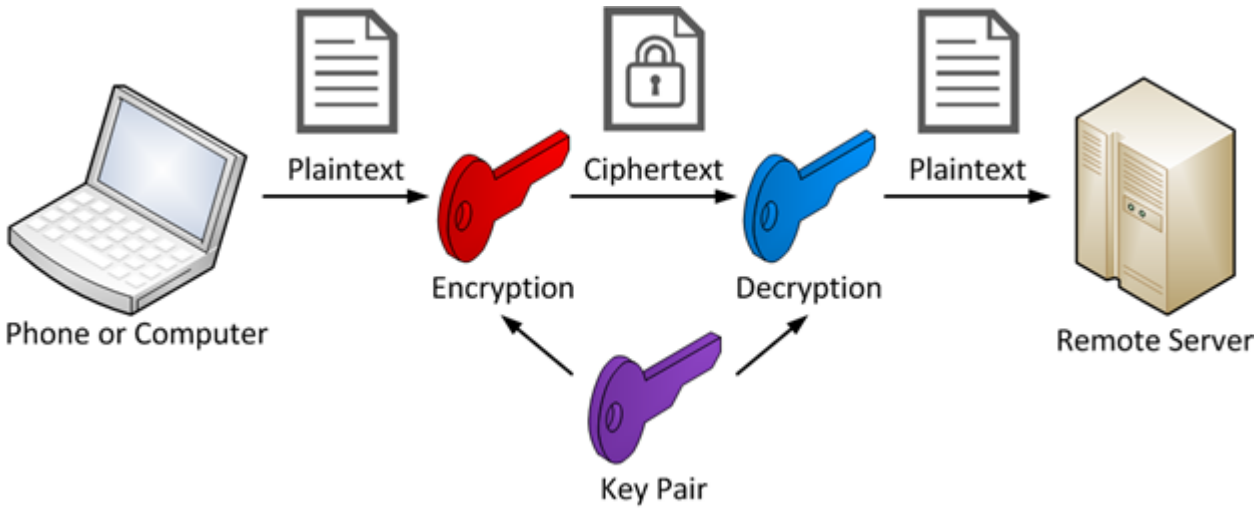
- How could we fix this? What do we wish we could do?

Alternatively

- I “sign” a contract with an HMAC and a key
- I give you the contract, the HMAC hash, and the key so you can verify the HMAC hash
- Problem?

Symmetric vs. asymmetric





Asymmetric cryptography

Encryption

- Public key: encrypt()
- Private key: decrypt()

Asymmetric cryptography

Digital signatures

- Public key: verify()
- Private key: sign()

Asymmetric cryptography

- Public key: not a secret
- Private key: must keep secret

Symmetric vs. asymmetric

- Symmetric: based on scrambling bits in ways we think provides confusion and diffusion
- Asymmetric: based on the difficulty of certain mathematical problems
- Both: outside of trivial cases (one-time pads), no proofs exist for their security

Symmetric vs. asymmetric

- Symmetric algorithms: Caesar cipher, substitution cipher, DES, 3DES, AES, etc.
- Asymmetric algorithms: RSA, DSA, ed25519 (elliptic curve)

Asymmetric algorithms

- Back to SnapTok
- I hard-code my public key into the app
- I use that to encrypt all of my users' data transmitted to my servers
- My servers have the private key
- Problem solved, right? Right!?

Why did we learn symmetric crypto?

- Asymmetric crypto is slow!
- You would need large keys to encrypt large messages!
- We still use symmetric crypto to encrypt everything
- But we use asymmetric crypto to handle the problem of symmetric key exchange

Why did we learn symmetric crypto?

- Asymmetric crypto is slow!
- You would need large keys to sign large messages!
- We still use hashes to hash everything
- But we use asymmetric crypto to handle the problem of authenticating the hash

Example from Assignment 6

https://brainhammer.com/cbc/?c=58d9f18eb1a68a928dc14ad17527f6bc04ddf9ca4aac64fb0aa83cdd5ab54c4185e8870321d3b24c78eb21057a961dad&iv=e486b3afb05e477d1ec8e2dae6efdc74&k=51905de251e6b496307787fd8104623a0bcdf895377ad56b42836c19db39f4b64f0f15008487a98db6e4183cc9ab001a8e3d09d1bb44c3553f8ccb27a76302279a4d02477eeea0a61c82039feefb0b85736c8de2a108066e483cafce7f2dff77a6958090a200355f786b45c5a92c3074c8f1a926bee2b6a85cb9c83d1c643116c971c429c3aaafcd0698f5f85b8097f8d157d492ec9bada481822398abf530e38b4ff7eb0248bb4cb6d3a6204a02236ffb28cb50af6c3ec63c7c880635431fe6e77855c2246a6b66c0339e78c97854fae550de47f2bf6b90076ce2d5e6aa1758d78afc9ff7c60ab88c8c727b2756c3090a6cb47c88bdb57d2c44b73d5b399239

Example from Assignment 6

- c=58d9f18eb1a68a928dc14ad17527f6bc04ddf9ca4aac64fb0aa83cdd5ab54c4185e8870321d3b24c78eb21057a961dad
- iv=e486b3afb05e477d1ec8e2dae6efdc74
- k=51905de251e6b496307787fd8104623a0bcdf895377ad56b42836c19db39f4b64f0f15008487a98db6e4183cc9ab001a8e3d09d1bb44c3553f8ccb27a76302279a4d02477eeea0a61c82039feefb0b85736c8de2a108066e483cafce7f2dff77a6958090a200355f786b45c5a92c3074c8f1a926bee2b6a85cb9c83d1c643116c971c429c3aaafcd0698f5f85b8097f8d157d492ec9bada481822398abf530e38b4ff7eb0248bb4cb6d3a6204a02236ffb28cb50af6c3ec63c7c880635431fe6e77855c2246a6b66c0339e78c97854fae550de47f2bf6b90076ce2d5e6aa1758d78afc9ff7c60ab88c8c727b2756c3090a6cb47c88bdb57d2c44b73d5b399239

Assignment 5

- Deadline: October 28, 2025, 10:00pm
- Real-world XSS attacks
  https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment5.pdf

Assignment 6

- Deadline: November 6, 2025, 10:00pm
- CBC padding oracle attacks
  https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment6.pdf